

Message

From: Moutsopoulos, Val (EHS) [val.moutsopoulos@massmail.state.ma.us]
Sent: 11/2/2012 9:55:11 PM
To: Hanchett, James (DPH) [/O=COMMONWEALTH OF MASSACHUSETTS/OU=MassMail-01/cn=Recipients/cn=James.Hanchett]
Subject: Security Bulletin: Spear Phishing Campaign (Email Attack)

EOHHS INFORMATION SECURITY BULLETIN

DATE ISSUED: November 2, 2012

SUBJECT: Possible spear phishing campaign (Email attack) to start on or after November 1, 2012

BACKGROUND: A report received from the Multi-State Information Sharing and Analysis Center warns of an email attack that may target State, Local, Tribal, and Territorial governments.

Spear phishing is an e-mail attack that targets a specific industry or organization, seeking unauthorized access to confidential data. This is usually conducted by perpetrators out for financial gain, trade secrets or government/military information.

Spear phishing messages appear to come from a trusted source. Messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In this case, however, the apparent source of the e-mail is likely to be an individual within the organization and generally someone in a position of authority.

This particular attack may originate from outside the country. If executed, the malicious files will execute a malicious piece of software to gain remote administrative access to your systems.

DETAILS:

The reported attack appears to be originating from webmaster@<U.S. State-level Department>.gov, and includes a malicious spreadsheet attachment "Details.xls".

ACTIONS:

We recommend the following:

- Do not open email attachments or click on URLs from unknown or untrusted sources.
- Check to make sure your antivirus software has the most recent updated signatures.
- Check to make sure your computer patches is up to date.
- If you believe you are experiencing an attack, please notify the Help Desk immediately.

REFERENCES:

Center for Internet Security

<http://www.cybergriffin.com/cyber-safety-tips/documents/CGSpearPhishingtipssheet.pdf>

United States Computer Emergency Readiness Team (US-CERT)

http://www.us-cert.gov/reading_room/phishing_trends0511.pdf

F-Secure

<http://www.f-secure.com/weblog/archives/ghostnet.pdf>

Anti-Phishing Working Group (APWG)

<http://www.antiphishing.org>

Thank you,

-Val

Val Moutsopoulos

IT Chief Security Officer

Executive Office of Health and Human Services

Commonwealth of Massachusetts

100 Hancock Street, Quincy, MA 02171

vmoutsop@state.ma.us

O: (617) 689-2823

C: 